

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

73B

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT AND
CRIMINAL COMPLAINT

I, Rachel Corn, being duly sworn, depose and state as follows:

1. This affidavit is submitted in support of an application for warrants to search the following locations (the "TARGET LOCATIONS"):

- a. The person of Shon Brian Beck;
- b. 2008 Advisory Court, Eldersburg, Maryland 21784;
- c. 2005 Silver Honda Civic, MD Tag 5AZC93;
- d. 2009 White Smart Car, MD Tag 5BG0383;
- e. The Google account associated with the email address shonbeck2@gmail.com;
- f. The Dropbox account associated with the email address shonbeck2@gmail.com and User ID 19014731;
- g. The Microsoft account associated with the email address shonbeck2@gmail.com; and
- h. The Microsoft account associated with the email address shon.beck@maryland.gov;

2. This affidavit is also made in support of a criminal complaint and arrest warrant for Shon Brian Beck, born in 1965, 2008 Advisory Court, Eldersburg, Maryland 21784, for violation of Title 18, United States Code, Section 2252A(a)(2) (receipt of child pornography).

3. I submit that there is probable cause to believe that the TARGET LOCATIONS will contain evidence of Title 18, United States Code, Section 2251(a) (production of child pornography), Title 18, United States Code, Section 2252A(a)(2) (distribution and receipt of child pornography), and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) (the "TARGET OFFENSES").

AGENT BACKGROUND

4. I am a Special Agent with the Federal Bureau of Investigation (FBI), Baltimore Division, Baltimore, Maryland. I have been a SA with the FBI since May 2006. Since September 2006, I have primarily investigated federal violations concerning child pornography and the sexual exploitation of children. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received FBI Crimes Against Children training, FBI Innocent Images Online Undercover training, and FBI Peer-to-Peer Network Online Investigation training. I have participated in the execution of numerous search warrants, of which the majority have involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violations of federal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A involving child exploitation offenses. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with the FBI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

5. The statements in this affidavit are based in part on information and reports provided by Maryland State Police (MSP) and Special Agents of the FBI, and on my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to

establish probable cause to believe I have set forth only the facts that I believe are necessary to establish probable cause to believe that Beck has committed criminal violations of 18 U.S.C. § 2252A(a)(2) (receipt of child pornography), and that evidence, fruits, and instrumentalities of the TARGET OFFENSES are located in the TARGET LOCATIONS.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO PRODUCE, POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE PRODUCTION, POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

6. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

h. I also know that the location of mobile phones can provide information about the individual's whereabouts, showing the places the holder resides or travels to, including the locations of additional digital devices that the individual possesses, controls, and has access to.

7. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were

somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence.

d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

e. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

f. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images,

videos, and other files. The data is maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account.

h. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

i. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the TARGET LOCATIONS notwithstanding the passage of time.

j. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

k. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

l. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

m. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

n. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

GOOGLE

8. Google provides numerous free services to the users with a Google profile. Some of services include, Gmail, Google Hangouts, Google Wallet, Google+, Google Drive, Picasa Web Albums, and YouTube. Gmail is a web-based email service that can also be accessed via mobile apps. In 2017, Gmail comes with 15GB of free storage and users can receive emails up to 50 megabytes in size, including attachments, while they can send emails up to 25 megabytes. In order to send larger files, users can insert files from Google Drive into the message. Emails remain in an active Gmail account until deleted by the user. Google Hangouts is a communication platform which includes instant messaging, video chat, and SMS and Voice Over IP (VOIP) features service that provides both text and voice communication. Google Hangouts allows conversations between two or more users. Chat histories are saved online, allowing them to be synced between devices. Google Wallet is a mobile payment system that allows its users to store debit cards, credit cards, loyalty cards and gift cards, among other things, on their mobile phones. Google+ is a social networking service. Google Drive is a file storage and synchronization service, which provides users with cloud storage, file sharing, and collaborative editing. Picasa Web Albums is an image hosting and sharing web service that allows users with a Google account to store and share images for free. YouTube is a free video sharing website that allows users upload, view and share videos.

MICROSOFT

9. Microsoft Account is a single sign-on service that allows users to log into Microsoft websites, devices, services, and applications, such as Hotmail, Xbox Live, Messenger and OneDrive. OneDrive, formerly known as SkyDrive, is a file hosting service that allows users to upload and sync files to a cloud storage and then access them from a Web browser or

their local device. OneDrive is part of a suite of online services offered by Microsoft and allows users to keep the files private, share them with contacts, or make them public. Microsoft Corporation is unable to provide OneDrive content, Calendar and Address Book/Buddy list content pursuant to a date range. Skype is a telecommunications application owned by Microsoft Corporation. Skype provides video chat and voice calls between one or more computers, tablets, mobile devices, Xbox consoles and smartwatches. Users can also exchange chat messages and share files.

DROPBOX

10. Dropbox is a file hosting service that offers “cloud” storage and file synchronization. Dropbox offers free and paid services that allow users to add photos, documents, videos and files to their account. Dropbox makes these files accessible to all of the user’s computers and mobile phones, and saves the files to the Dropbox server, so they may be accessed from anywhere. Dropbox offers a free plan that allows users to have 2GB of space to store their files. Dropbox also offers additional space on the Dropbox servers for a fee.

11. According to Dropbox’s privacy policy, at <https://www.dropbox.com/privacy>, Dropbox collects and stores the files users upload and delete and also collects logs. Dropbox records when the user uploads and deletes a file but Dropbox does not record when the user downloads a file. Dropbox collects and associates a user’s account with their name, email address, phone number, payment info, physical address, and account activity. Dropbox collects information related to how users use their Services, including actions users take in their account, like sharing, editing, viewing, and moving files or folders. Dropbox also collects information from and about the devices users use to access their Services. This includes things like IP addresses, the type of browser and device used, the web page visited before coming to Dropbox

sites, and identifiers associated with the users' devices.

12. In order to create a Dropbox account, a user is required to register with an email address. Once registered, each user is assigned a unique user ID. Dropbox communicates with users via stored email accounts on file when users access and make changes to their accounts unless the user opts-out of those emails. To sign into the user's Dropbox account, the user enters their email and password. Once a user has a Dropbox account, they can invite other Dropbox users to access their shared folders. A shared folder is one in which more than one user has access to, and can add, download or delete content. If a user joins another user's shared folder, the shared folder size counts towards the first user's space limitation. If a user is invited to join another user's folder, the invitation request is sent to the registered email account. A user can share their login information for an account, therefore more than one person could plausibly take actions in the Dropbox account at the same time, but it would all appear as the same user to Dropbox.

13. Dropbox maintains IP addresses for web-based logins and the last-seen IP address of linked computers. IP address information is typically maintained for 6 months. IP addresses of specific actions within a Dropbox account, such as uploads and deletions, are not available. Additionally, if a user is accessing files in their Dropbox account from a desktop or mobile application, that access may not be logged by Dropbox

PROBABLE CAUSE

14. In October 2018, [REDACTED] Jane Doe 1, born in 1996, disclosed that Beck sexually abused her and filmed the abuse when she was a child. Jane Doe 1 advised that the abuse and recording of the abuse [REDACTED]
[REDACTED]

[REDACTED] Jane Doe 1 also advised that [REDACTED] told her she “caught” Beck “viewing or reading” child pornography in approximately 2000 or 2001. In December 2018, Jane Doe 1 received an unsolicited email from Beck’s known email account, **shonbeck2@gmail.com**. The email asked for “forgiveness,” and did not explicitly state what the forgiveness was for. Jane Doe 1, with the assistance of investigators, responded to Beck and stated that Beck had sexually abused her, and told Beck to “own up.” Beck responded in early January, and stated that he did not sexually abuse Jane Doe 1.

15. On May 22, 2019, Investigators from the MSP and the FBI executed a state search and seizure warrant at the residence of Beck located at **2008 Advisory Court, Eldersburg, Maryland 21784**. I was present for the execution of the search warrant. The state search warrant was authorized to search for evidence of Child Porn Film/Comp Sex Act, Section CR 11-207(a)(2)(3), Sex Abuse Minor – Continuing Course of Conduct, Section CR 3-315, Possess Child Porn, Section CR 11-208, Human Trafficking – Guardian, Section CR 11-303(b)(1). During the execution of the search warrant, Beck, his wife, and their son, born in 2000, were present. The house was very cluttered and disorganized.

16. During the execution of the search warrant, numerous digital items, including an Acer Aspire desktop computer and a Lexar Media Compact Flash 8MB Card were located and seized. The desktop computer was located in the front office and the flash card was located in the basement.

17. During the execution of the search warrant, Beck waived his Miranda rights and consented to an interview, which was audio recorded. I participated in the interview with an investigator from the MSP. Beck advised that his computer was the Acer Aspire desktop computer located in the front office of the residence. Beck stated he had a “porn problem” and

that he views pornography almost daily. Beck stated that he visits the website “jpg4.us” to view pornography, and that he has seen child pornography on that website. Beck said that his daughter once looked over his shoulder and saw the pornography that he was viewing, which Beck described as naked teenagers on a beach. When asked if he had a “go to” or “favorite” porn, Beck replied, “It’s incest porn. But I mean you but the actual the thought of doing it’s kind of disgusts me but for some reason where someone else is doing it, it excites me.” When asked if he reads any child pornography stories, Beck replied “just the incest ones,” and later stated that he saved the incest stories to his computer, and added, “but I’m not big in reading. I’m really not. I don’t like reading.” Beck denied sexually abusing Jane Doe 1 and stated, “that’s disgusting,” and also denied taking any naked or sexual pictures or videos of Jane Doe 1. Beck initially denied saving any child pornography, but later stated that there “might” be child pornography on his computer. Beck then admitted to “looking at that stuff,” but immediately added that he did not “touch or anything like that to” Jane Doe 1. Beck stated he used a “screen capture utility” to save pornography, to include child pornography, to his “E” drive on his computer. Beck stated he did not know why he saved the child pornography. Beck denied using encryption but stated he used programs such as Eraser¹ and CCleaner.² Beck denied sending or receiving child pornography files through email, text, or any application. Beck stated that his email addresses were **shon.beck@maryland.gov** and **shonbeck2@gmail.com**.

18. After the execution of the search warrant, Beck resided with friends, and his wife and son continued to live at **2008 Advisory Court, Eldersburg, Maryland 21784**. Over time,

¹ Eraser is an advanced security tool for Windows which allows users to completely remove sensitive data from the user’s hard drive by overwriting it several times with carefully selected patterns.

² CCleaner is a utility used to clean potentially unwanted files and invalid Windows Registry entries from a user’s computer.

Beck visited 2008 Advisory Court, Eldersburg, Maryland 21784 to help clean out the residence so he and his wife could sell the house. After the execution of the search warrant and the seizure of Beck's phone, Beck's wife provided Beck with one of her cell phones for his use.

19. The Acer Aspire desktop computer was forensically examined and the results revealed hundreds of images saved on the E drive, including child pornography, child erotica, and anime. Many of the images had titles that began with "Capture" which is the default naming convention for the Window's program "Snipping Tool."³ Two of the images are described as follows:

- a. "Capture1rrr.jpg" (created date of May 16, 2019): Depicts a prepubescent female performing oral sex on an adult male; and
- b. "Capture1pppppp.jpg" (created date of May 16, 2019): Depicts a naked prepubescent female laying on her back with her legs bent and spread opened and her genitalia exposed to the camera. The female's hands are touching her genitalia.

Based on my training and experience, I have concluded that these two image files contain visual depictions of minors engaging in sexually explicit conduct and are child pornography under 18 U.S.C. § 2256(8).

20. The forensic examination of the Acer Aspire desktop computer also revealed Chrome Autofill⁴ data. The email addresses saved as an autofill entry were **shonbeck2@gmail.com** and **shon.beck@maryland.gov**. The forensic examination of the Acer Aspire desktop computer also contained information regarding Cloud Service programs for **Dropbox** and **OneDrive**.

³ Snipping Tool is a Microsoft Windows screenshot utility included in Windows Vista and later. The tool can take still screenshots of an open window, rectangular areas, a free-form area, or the entire screen.

⁴ Chrome Autofill enables users to store certain data, like their name, address, email address, or phone number, as an Autofill entry. A user can then use this data to automatically fill in forms online. A user can store multiple addresses and email addresses as separate entries.

21. The forensic examination of the Lexar Media Compact Flash 8MB Card revealed numerous deleted files. Some of the deleted files appeared to be pictures of Jane Doe 1 as a young child at family events, such as a baby shower and the Baltimore Aquarium. Approximately 11 images depicted a prepubescent female who appears to be sleeping on her side with her back to the camera. The pillow case depicted in one of the pictures contains what looks like a red, pink and orange flower. The girl is wearing what appears to be a green nightgown and “Rugrats” underwear. In approximately 9 of the images, an adult hand is moving the girl’s underwear and exposing her genitalia and/or buttocks to the camera. In approximately 7 of the 9 pictures, a ring is observed on the finger of the adult hand. In one picture, the ring appears to have diamonds in it. The EXIF metadata within the 11 images revealed that the images were taken with an Epson Digital Still Camera on September 21, 2001.

22. In October 2019, some of the deleted images from the Lexar Media Compact Flash Card were shown to Beck’s wife. Beck’s wife stated she did not recognize the pillow case and did not recognize the background from the pictures with the sleeping girl. Beck’s wife stated that the ring depicted in the image looks like Beck’s second, and most current, wedding band.

23. In November 2019, Beck’s wife advised investigators that she saw Beck and he was still wearing his wedding band and that she thought it was the same ring depicted in the image that was shown to her in October 2019. In December 2019, Beck’s wife advised that Beck moved back into **2008 Advisory Court, Eldersburg, Maryland 21784**, and resided in the basement. In January 2020, Beck’s wife advised that she moved out of **2008 Advisory Court, Eldersburg, Maryland 21784**, and a few weeks later she advised that her son also moved out, and that Beck continued to reside there by himself. In February 2020, **2008 Advisory Court**,

Eldersburg, Maryland 21784 was listed for sale. Beck's wife stated that much of the property has been removed from the residence, but she believes there are a few of their personal items remaining. These items include movie equipment and a computer in the basement, Beck's clothing and other personal belongings in a bedroom where he is sleeping, and various items in the garage.

24. On March 3, 2020, Beck's wife advised that she recently found pictures in one of her old scrapbooks of a trip her family took with her coworkers on September 21, 2001 (the same day that the series of 11 deleted images described in paragraph 21 above were produced). Beck's wife advised that her family and two other families stayed in a townhouse in Bethany Beach, Delaware. In the scrapbook there is a picture of her coworker's daughter, Jane Doe 2, who is wearing a green nightgown with a Rugrats character on it. The green nightgown appears to be the same color green as the nightgown worn by the girl depicted in the deleted images found on the Lexar Media Compact Flash Card.

25. On March 3, 2020, Beck's wife also advised that she found a picture of Beck's wedding ring in her son's baby scrapbook. The picture is a close up of Beck's hand with their baby son touching his index finger. The wedding band is depicted and although there is not sufficient detail to make a positive identification, it appears to be similar to the ring depicted in the deleted images found on the Lexar Media Compact Flash Card.

26. Beck's wife also confirmed that she saw Beck in person on March 3, 2020 and he was still wearing the wedding band.

27. Maryland Motor Vehicle records reflect that Beck owns 4 Vehicles, including a **2005 Silver Honda Civic, MD Tag 5AZC93** and a **2009 White Smart Car, MD Tag 5BG0383**. Both of these vehicles were present at the residence at the time of the search warrant

execution on May 22, 2019. On March 2, 2020, Beck's wife advised that although in the past Beck rarely drove the **2005 Silver Honda Civic**, she noticed a week prior that the **2005 Silver Honda Civic** was not at **2008 Advisory Court, Eldersburg, Maryland 21784**. When she asked Beck about the car, he told her that he found a place to store the car. Beck's wife also stated that when she last observed the **2005 Silver Honda Civic** in either late February 2020 or early March 2020, she observed clothes in a bag and "other random stuff" in the backseat of the car.

28. On March 6, 2020, the mother of Jane Doe 2 was interviewed. She advised that she went on a trip to Bethany Beach, Delaware, with the Beck family and other coworkers, although she could not recall the exact date of the trip. Jane Doe 2's mother advised that she brought her two minor children on the trip. Jane Doe 2's mother was shown one of the series of 11 deleted images described in paragraph 21 above from the Lexar Media Compact Flash Card and immediately recognized her youngest daughter in the image. Jane Doe 2 was born in 1995, and would have been 6 years old on September 21, 2001. Jane Doe 2's mother also recognized the pillow and the pink blanket depicted in the image, which both belonged to her family.

29. On March 6, 2020, and on March 9, 2020, surveillance was conducted at **2008 Advisory Court, Eldersburg, Maryland 21784**. At approximately 5:37 am and 5:34 am respectively, the right garage door opened and a **white Smart car**, bearing a **Maryland tag 5BG0383**, was observed pulling out of the garage and driving away from the house. The **2009 white Smart car**, bearing a **Maryland tag 5BG0383**, is registered to **Shon Brian Beck, 2008 Advisory Court, Eldersburg, Maryland 21784**.

30. An administrative subpoena was sent to Google for subscriber information for the account associated with **shonbeck2@gmail.com**. Google provided the following information regarding the account:

Name: Shon Beck
Recovery Email: **shon.beck@maryland.gov**
Created On: 05/04/2005
SMS: 443-250-5990

31. An administrative subpoena was sent to Dropbox for subscriber information for the account associated with **shonbeck2@gmail.com**. Dropbox provided the following information regarding the account:

Name: Shon Beck
User ID: **19014731**
Account Status: Active
Subscription Status: Free
Account Creation Date: 01/18/2011

32. An administrative subpoena was sent to Microsoft for subscriber information for the account associated with **shonbeck2@gmail.com**. Microsoft provided the following information regarding the account:

State: Illinois
Services Utilized: Mail and Microsoft Support
Creation Date: 08/22/2007
Last Modified Date: 10/29/2019 for Microsoft Support

33. An administrative subpoena was sent to Microsoft for subscriber information for the account associated with **shon.beck@maryland.gov**. Microsoft provided the following information regarding the account:

Name: Shon Beck
Services Utilized: Mail
Creation Date: 07/26/2016

REQUEST FOR AUTHORIZATION TO EXECUTE
SEARCH WARRANT ANYTIME

34. Based on the facts set forth above, I believe that Beck drives the Smart Car and that Beck may leave his residence to go to his employment prior to 6:00 am. It is respectfully requested that this Court provide the authorization to execute the search warrants as early as 5:00

am. Executing the warrants before Beck exits the residence will be safer for law enforcement and less invasive to Beck and the other occupants of the residence.

35. Because warrants will be served on Google, Dropbox, and Microsoft Corporation, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

SUMMARY

36. Based on my training and experience and the fact set forth above, including the images located on the desktop computer and Lexar Media Card, I believe that Shon Brian Beck displays characteristics common to individuals who have a sexual interest in children, and who access with the intent to view and/or, possess, collect, receive, and distribute child pornography as discussed in paragraphs 6 and 7 above.

37. Based on my training, knowledge and experience, individuals who have a sexual interest in children and who receive and possess child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for many years – even decades. These individuals go to great lengths to conceal and protect their collection from discovery, theft, and damage. Individuals who collect child pornography prefer not to be without their child pornography for any prolonged time period and therefore they tend to keep their collection where they can easily access it such as in their residence, vehicles and place of employment, as well as on their person. Individuals who collect child pornography also tend to keep their collection on multiple devices, many of which are portable such as a smartphone, laptop computer, and external storage devices, such as flash drives, external hard drives, and other storage media. In my investigative experience, as well as the documented experience of other investigators, these devices are often


kept in the individuals' homes, vehicles, place of employment and on their person.

38. Based on these characteristics, and because the Google, Dropbox, and Microsoft accounts appear to be accessed and controlled by Beck, I respectfully submit there is probable cause that the Google, Dropbox, and Microsoft accounts contain evidence (1) of receipt, and/or possession of child pornography, and (2) are relevant to determine the ownership and control of the accounts and the ownership of the desktop computer and Lexar Media Card seized from Beck's residence. Based on my training and experience, such information may constitute evidence of the TARGET OFFENSES because the information can be used to identify the account's user or users.

CONCLUSION

39. Based upon the foregoing information set forth in this application, I respectfully submit that there is probable cause to believe that Shon Brian Beck, violated Title 18, United States Code, Section 2252A(a)(2) (receipt of child pornography).

40. Also, based on the foregoing information, I have probable cause to believe that contraband, evidence, fruits, and instrumentalities of the TARGET OFFENSES as set forth herein and in Attachments B1, B2, B3, B4, B5, B6, and B7, are currently contained in the TARGET LOCATIONS, more fully described in Attachments A1, A2, A3, A4, A5, A6, and A7. I therefore respectfully request that search warrants be issued authorizing the search of the locations described in Attachments A1, A2, A3, A4, A5, A6, and A7, for the items described in Attachments B1, B2, B3, B4, B5, B6, and B7, and authorizing the seizure and examination of any such items found therein.


Special Agent Rachel S. Corn
Federal Bureau of Investigation

Subscribed and sworn to before me this 18 day of March 2020.



HONORABLE J. MARK COULSON
UNITED STATES MAGISTRATE JUDGE